UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/987,912	11/16/2001	Mark Crosbie	10012172	7899

7590 03/02/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
DODDS, HAROLD E	

ART UNIT	PAPER NUMBER
2168	

DATE MAILED: 03/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/987,912	CROSBIE ET AL.	
	Examiner	Art Unit	
	Harold E. Dodds, Jr.	2168	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20,22 and 23* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20,22 and 23* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 22, and 23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The phrase "storing system call parameters or data the parameters" on line 2 of each of the these claims is indefinite. What data is referred to in the phrase "or data"? Does this mean system data or system call data? Please amend these claims to provide more definite language.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-16, 18-20, and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Crosbie et al. (U.S. Patent Application Publications No. US 2002/0083343).

The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

5. Crosbie anticipated independent claim 1 by the following:

"...storing system call parameters or data the parameters point to at the beginning of a system call..." at p. 10, par. 0205.

"...enabling the generation of audit data when a device driver is opened for read, and halting data generation when the device driver is closed..." at p. 9, par. 0174.

"...and triggering data delivery at the end of a system call path..." at p. 10, par. 0205.

"...and generating an audit record and depositing the audit record in a circular buffer..." at p. 10, par. 0205

6. As per claim 2, the "...for each system call that accesses files, storing related file information...," is taught by Crosbie at p. 10, par. 0205.

7. As per claim 3, the "...related file information includes file owner or group and the file information is stored before any modifications occur that might affect the file information...," is taught by Crosbie at p. 10, par 0205.

8. As per claim 4, the "...system call parameters that include path name parameters are stored with full path name information..." is taught by Crosbie at p. 12, par. 0237-0239.

9. As per claim 5, the "...audit record is a tokenized audit record...," is taught by Crosbie at p. 7, par. 0138.

10. As per claim 6, the "...reading audit records from the circular buffer...," is taught by Crosbie at p. 7, par. 0138.

11. As per claim 7, the "...reading is triggered using a device read call...," is taught by Crosbie at p. 10, par 0205.

12. As per claim 8, the "...maintaining system wide configuration related data structures...," is taught by Crosbie in Figure 3,

the "...and setting selection masks based on such structures...," is taught by Crosbie at p. 21, par. 0761,

and the "...for specifying data to be delivered...," is taught by Crosbie at p. 8, par. 0155.

13. As per claim 9, the "...collecting data in the system call path...," is taught by Crosbie p. 10, par. 0205 and p. 18, par. 0610,

and the "...and formatting the collected data into an audit record...," is taught by Crosbie at p. 6, par. 0105.

14. As per claim 10, the "...collected data is a token stream...," is taught by Crosbie at p. 7, par. 0138.

15. As per claim 11, the "...if the circular buffer is full, then either reading some of the audit records from the circular buffer or dropping new records until space becomes available in the circular buffer..." is taught by Crosbie at p. 9, par. 0175.

16. As per claim 12, the "...maintaining root and current directories while threads are in the middle of system call processing...," is taught by Crosbie at p. 12, par. 0239.

17. As per claim 13, the "...selecting which data to collect before said collecting step...," is taught by Crosbie at p. 21, par. 0761 and p. 6, par. 0105.

18. As per claim 14, the "...said selecting step can be based on process, user, group, filename information and/or time intervals...," is taught by Crosbie at p. 10, par. 0205.

19. As per claim 15, the "...detecting hard link accesses to a critical file...," is taught by Crosbie at p. 18, par. 0616.

20. As per claim 16, the "...maintaining a critical file list for monitoring hard links...," is taught by Crosbie at p. 16, par. 0451-0461 and p. 18, par. 0616.

21. As per claim 18, the "...said selecting step can be based on an outcome of system calls including pass, failure or both...," is taught by Crosbie at p. 14, par. 0347.

22. As per claim 19, the "...presenting deposited delivered data to a user space via a device driver in the kernel..." is taught by Crosbie at p. 10, par. 0205.

23. As per claim 20, the "...configuring which system calls are audited by making ioctl() (control) calls on a device driver...," is taught by Crosbie at p. 9, par. 0171.

24. As per claim 22, the "...storing system call parameters or data the parameters point to at the beginning of a system call...," is taught by Crosbie at p. 10, par. 0205,

the "...triggering data delivery at the end of a system call...," is taught by Crosbie at p. 10, par. 0205,

the "...and generating an audit record and depositing the audit record in a circular buffer...," is taught by Crosbie at p. 10, par. 0205,

the "...selecting data to be collected based on an outcome of a system call including pass, failure or both...," is taught by Crosbie at p. 14, par. 0347,

and the "...and collecting data in the system call and formatting the collected data into an audit record....," is taught by Crosbie at p. 10, par. 0205 and p. 18, par. 0610.

Allowable Subject Matter

25. Claim 23 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action.

26. Claim 17 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

Response to Arguments

27. Applicants' arguments filed 22 December 2005 have been fully considered but they are not persuasive. In the first argument for independent claim 1 on page 7, paragraph 5, the Applicants state:

"The Examiner has failed to identify with specificity where Crosbie discloses enabling the generation of audit data when a device driver is opened for read and halting data generation when the device driver is closed. Paragraph 205 of Crosbie states that "a read () of /dev/idds [forces] the IDDS kernel driver 370 to read the next audit record block from the circular buffer." Thus, a read () causes the driver 370 to read the next audit record without specifying enabling the audit data generation and halting data generation based on the device driver opening/closing, respectively, as claimed. For at least this reason, the rejection of claim 1 should be withdrawn."

The Examiner disagrees. Crosbie states the opening and reading of the IDDS driver as follows:

"...The idskerndsp 240 will **open the driver device** and send configuration data to the kernel. The idskerndsp 240 will **read audit records** in blocks from this device..." at p. 9, par. 0174.

This reference teaches the opening of the device and the reading of audit records. It is inherently understood that a device the may be opened must also be closed and that reads may be made to the device only during the period that it is opened.

28. In the second argument for claim 2 on page 8, paragraph 2 the Applicants state:

"With specific reference to claim 2, Crosbie fails to disclose storing related file information for each system call accessing files. Crosbie at paragraph 205 states that system call header related information is gathered. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 2 should be withdrawn."

Crosbie explicitly teaches the storing of specific information as follows:

"If the system call is being audited, the initial component of the syscall handler gathers some header related information: user id, group id, timestamps, process id, etc. At step 315 as the system call is processed, **information is stored** in temporary buffers..." at p. 10, par. 0205.

27. In the third argument for claim 8 on page 8, paragraph 3 the Applicants state:

"With specific reference to claim 8, Crosbie fails to disclose setting selection masks based on system wide configuration related data structures for specifying data to be delivered as claimed in amended claim 8. Paragraph 761 of Crosbie states that trace and log message generation is controlled by setting of a command line argument. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 8 should be withdrawn."

The Examiner disagrees. Crosbie teaches the selection of data using masks and the delivery of data as follows:

"...The user can **select** what elements of the ECS engine core operation to trace using the tracing value as a **bit mask...**" at p. 21, par. 0761.

"...For example, **kernel audit data, syslog records or login records are all delivered** to the engine as events..." at p. 8, par 0155.

When combined these two citations the user uses bit masks to select which of the data events will be delivered. The second citation (p. 8, par. 0155) describes the types of data which might be selected.

28. In the fourth argument for claim 9 on page 8, paragraph 4 the Applicants state:

"With specific reference to claim 9, Crosbie fails to disclose formatting collected data into an audit record. Crosbie at paragraph 105 states that "[a] set of data gathering components . . .provides a way of observing what activity is occurring on the systems and networks" without disclosing the collecting data in a system call path and formatting the collected data into an audit record. The Examiner is requested to specifically identify where in the reference the Examiner believes the claimed limitation is to be found. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 9 should be withdrawn.

The Examiner disagrees. Crosbie teaches the use of system calls at p. 10, par. 0205 and the use of call paths at p. 18, par. 0610. Crosbie teaches the collection (gathering) and formatting of data as follows:

"...A set of data gathering components which use kernel **audit data** 70 and system log data 72 provides a way of observing what activity is occurring on the systems and networks. This is accomplished through a set of **data gathering modules that gather and format information** from data sources at various points within the system..." at p. 6, par. 0105.

The gathering and formatting of audit data produces audit records.

29. In the fifth argument for claim 10 on page 8, paragraph 5 the Applicants state:

"Similar to claim 9, with specific reference to claim 10, Crosbie fails to disclose that the collected data is a token stream. The Examiner is requested to specifically identify where in the reference the Examiner believes the claimed limitation is to be found. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 10 should be withdrawn."

The Examiner disagrees. Crosbie teaches this limitation as follows:

"...It uses a meta-description language (MDL) to define what a record in a data stream looks like..." at p. 7, par. 0138.

This teaching describes the construction of token streams.

30. In the sixth argument for claim 13 on page 8, paragraph 6 the Applicants state:

"With specific reference to claim 13, Crosbie fails to disclose a selecting step for selecting which data to collect before the collecting step. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step is disclosed. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 13 should be withdrawn."

The Examiner disagrees. Crosbie teaches this limitation as follows:

"...The user can **select** what elements of the ECS engine core operation to trace using the tracing value as a **bit mask**..." at p. 21, par. 0761.

"...A set of data gathering components which use kernel **audit data** 70 and system log data 72 provides a way of observing what activity is occurring on the systems and networks. This is accomplished through a set of **data gathering modules that gather and format information** from data sources at various points within the system..." at p. 6, par. 0105.

These two references when combined teach the selecting occurring for the collection (gathering) step.

31. In the seventh argument for claim 14 on page 8, paragraph 7 and page 9, paragraph 1 the Applicants state:

"With specific reference to claim 14, Crosbie fails to disclose that the selecting step is based on process, user, group, filename information and/or time intervals. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step based on process, user, group, filename information and/or time intervals is disclosed. For at least this reason and for those advanced above with respect to claim 1, the rejection of claim 14 should be withdrawn."

The Examiner disagrees. Claim 14 is essentially the same as claim 2 and the response to second argument applies to the seventh argument

32. In the eighth argument for claim 18 on page 9, paragraph 2 the Applicants state:

"With specific reference to claim 18, Crosbie fails to disclose a selecting step based on an outcome of system calls including pass, failure, or both. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step based on process, user, group, filename information and/or time intervals is disclosed. For at least this reason arid for those advanced above with respect to claim 1, the rejection of claim 18 should be withdrawn.

The Examiner disagrees. Claim 18 has the limitation "said selecting step can be based on an outcome of system calls including pass, failure or both". The remaining portion of this argument is not related to the limitation in claim 18. Crosbie teaches this limitation as follows:

"...This template collects information from /var/adm/sulog. This log is used to detect failed su attempts..." at p. 14, par. 0347.

This teaching provides an example of a system call, which results in failure. In a system the absence of a failure is a pass. Therefore, the selection may be made on the outcome of a system call being either a failure of a pass. The "or both" option means that no selection is being made according to this criterium.

33. In the ninth argument for new independent claim 22 on page 9, paragraph 3 the Applicants state:

"Further, new claim 22 is patentable over Crosbie as Crosbie fails to.disclose at least a selecting step which is based on an outcome of system calls including pass, failure, or both. Contrary to the Examiner's assertion regarding claim 18 (hereby incorporated into claim 22), paragraph 205 of Crosbie fails to disclose a selecting step for selecting which data to collect before the collecting step. The Examiner is requested to identify with specificity where in paragraph 205 of the reference, the Examiner believes the selecting step (and selecting step based on the outcome of system calls including pass, failure, or both) is disclosed. Because the claimed limitation of at least selecting which data to collect before the collecting step is not found in Crosbie, claim 22 is believed to be patentable over Crosibie."

The Examiner disagrees. This new independent claim incorporated the limitation, which is used in dependent claim 18. As such, the response to eighth argument also applies to the ninth argument.

34. In the tenth argument for new independent claim 23 on page 9, paragraph 4 the Applicants state:

"New claim 23 recites a method of generating kernel audit data comprising: storing system call parameters or data the parameters point to at the beginning of a system call; and triggering data delivery at the end of the system call and generating an audit record and depositing the audit record in a circular buffer if, based on the success or failure of the system call, auditing of the system call should continue as specified in a post-call selection flag. The method of new claim 23 is not disclosed by Crosbie and is patentable over Crosbie."

The examiner agrees in part. Crosbie does not teach the use of a post-call selection flag. The remaining limitations are addressed in the responses to the seventh and ninth arguments.

Conclusion

35. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Harold E. Dodds, Jr. whose telephone number is (571)-272-4110. The examiner can normally be reached on Monday - Friday 8:00 - 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey A. Gaffin can be reached on (571)-272-4146. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Harold E. Dodds. Jr.
Patent Examiner
February 28, 2006